IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 – 2 (Canceled)

3. (Currently Amended) A method for analyzing a logfile produced by a computer network security system, comprising:

providing a regular expression query associated with a pattern to be searched for in the logfile; and

using the query to search for the pattern in the logfile;

wherein the pattern is associated with a sgid (set group ID) exploit in which a sgid process is used to spawn another process and using the query to search for the pattern includes searching for entries showing that a process has been started by a sgid process with effective group ID equal to zero and group ID (gid) not equal to zero.

4. (Original) The method as recited in claim 3, wherein using the query to search for the pattern further includes storing a process ID of the process, and searching for processes with a parent process ID equal to the stored process ID.

5 – 8 (Canceled)

9. (Currently Amended) A method for analyzing a logfile produced by a computer network security system, comprising:

providing a regular expression query associated with a pattern to be searched for in the logfile; and

using the query to search for the pattern in the logfile;

wherein the pattern is associated with a sgid (set group ID) exploit in which a sgid process is used to spawn another process, the pattern is associated with processes spawned by a

shell, and using the query to search for the pattern includes searching for entries showing that the shell has started a process, storing a process ID of the process, and searching for entries showing processes with parent process ID equal to the stored process ID;

wherein the shell comprises a sgid process with effective group ID equal to zero and group ID (gid) not equal to zero.

10 - 28 (Canceled)

29. (Currently Amended) A system for analyzing a logfile produced by a computer network security system, comprising:

a storage including a regular expression query associated with a pattern to be searched for in the logfile; and

a processor configured to use the query to search for the pattern in the logfile;

wherein the pattern is associated with a sgid (set group ID) exploit in which a sgid process is used to spawn another process and the processor is further configured to search for entries showing that a process has been started by a sgid process with effective group ID equal to zero and group ID (gid) not equal to zero.

30. (Original) The system as recited in claim 29, wherein the processor is further configured to store a process ID of the process, and search for processes with a parent process ID equal to the stored process ID.

31 – 34 (Canceled)

35. (Currently Amended) A computer program product for analyzing a logfile produced by a computer network security system, comprising a computer usable medium having machine readable code embodied therein for

providing a regular expression query associated with a pattern to be searched for in the logfile; and

using the query to search for the pattern in the logfile;

wherein the pattern is associated with a sgid (set group ID) exploit in which a sgid process is used to spawn another process and using the query to search for the pattern includes searching for entries showing that a process has been started by a sgid process with effective group ID equal to zero and group ID (gid) not equal to zero.

36 – 41 (Canceled)

INTERVIEW SUMMARY UNDER 37 CFR §1.133 AND MPEP §713.04

A telephonic interview in the above-referenced case was conducted on 5/16/05 between the Examiner and the Applicants' undersigned representative. The Office Action mailed on 2/22/05 was discussed. Specifically, the rejections of claims 3, 4, 9, 29, 30 and 35 in light of Crosbie et al, "IDIOT – Users Guide" (Technical Report TR-96-050, Perdue University, September 4, 1996) and the proposed amendments set forth herein were discussed with the intent to place the claims in better condition for allowance or appeal. Although no agreement was reached regarding the claims, the Examiner indicated the claims may be allowable over the references cited to date if they were amended to further define the recited "sgid exploit". The Applicants wish to thank the Examiner for his time and attention in this case.